Accusé de réception de la préfecture en date du mercredi 6 juin 2018

DEPARTEMENT
DES
DEUX-SEVRES

VILLE DE NIORT

EXTRAIT DU REGISTRE DES DELIBERATIONS DU CONSEIL MUNICIPAL

SEANCE DU 4 JUIN 2018

Délibération n° D-2018-186

Utilisation du service FranceConnect pour l'authentification des usagers des services numériques de la Ville de Niort

Conseillers en exercice : 45

Votants : 43

Convocation du Conseil Municipal :
le 29/05/2018

Affichage du Compte-Rendu Sommaire et affichage intégral :
le 11/06/2018

Président :
MONSIEUR JÉRÔME BALOGE

Présents :

Monsieur Jérôme BALOGE, Monsieur Marc THEBAULT, Madame Rose-Marie NIETO, Monsieur Alain BAUDIN, Madame Christelle CHASSAGNE, Monsieur Alain GRIPPON, Madame Jacqueline LEFEBVRE, Monsieur Michel PAILLEY, Madame Dominique JEUFFRAULT, Monsieur Luc DELAGARDE, Madame Anne-Lydie HOLTZ, Monsieur Lucien-Jean LAHOUSSE, Madame Jeanine BARBOTIN, Monsieur Dominique SIX, Madame Sylvette RIMBAUD, Madame Elisabeth BEAUVAIS, Madame Marie-Paule MILLASSEAU, Madame Catherine REYSSAT, Monsieur Dominique DESQUINS, Madame Cécilia SAN MARTIN ZBINDEN, Monsieur Eric PERSAIS, Madame Agnès JARRY, Madame Yvonne VACKER, Monsieur Elmano MARTINS, Monsieur Guillaume JUIN, Madame Christine HYPEAU, Madame Marie-Chantal GARENNE, Monsieur Florent SIMMONET, Madame Valérie BELY-VOLLAND, Madame Yamina BOUDAHMANI, Monsieur Romain DUPEYROU, Monsieur Simon LAPLACE, Monsieur Nicolas ROBIN, Madame Josiane METAYER, Monsieur Pascal DUFORESTEL, Madame Elodie TRUONG, Monsieur Jacques TAPIN, Madame Isabelle GODEAU, Madame Monique JOHNSON, Monsieur Jean-Romée CHARBONNEAU.

Secrétaire de séance : Yvonne VACKER

Excusés ayant donné pouvoir :

Monsieur Fabrice DESCAMPS, ayant donné pouvoir à Madame Rose-Marie NIETO, Madame Carole BRUNETEAU, ayant donné pouvoir à Monsieur Jérôme BALOGE, Monsieur Alain PIVETEAU, ayant donné pouvoir à Madame Monique JOHNSON

Excusés :

Madame Fatima PEREIRA, Madame Nathalie SEGUIN.

CONSEIL MUNICIPAL DU 4 juin 2018

Délibération n° D-2018-186

Direction des Systèmes d'Information et de Télécommunications

Utilisation du service FranceConnect pour l'authentification des usagers des services numériques de la Ville de Niort

Monsieur Lucien-Jean LAHOUSSE, Adjoint au Maire expose :

Mesdames et Messieurs,

Après examen par la commission municipale compétente

Sur proposition de Monsieur le Maire

Dans le cadre de la mise en place de services numériques pour faciliter les démarches administratives des usagers, la Ville de Niort souhaite utiliser le service FranceConnect comme un des moyens d'authentification des usagers.

A ce titre, les services utilisant l'authentification par FranceConnect disposent d'un simple onglet « S'identifier avec FranceConnect ».

Le service FranceConnect fédère les identités numériques des usagers et permet :

- aux usagers de bénéficier d'une chaîne de confiance facilitant l'accès aux différents services numériques, de garantir la confidentialité des informations et d'utiliser un même compte d'accès pour effectuer leurs démarches en ligne auprès de diverses entités ;
- à la Ville de Niort de déléguer la gestion des identités numériques et l'authentification des usagers à des tiers de confiance fournisseurs d'identité.

Les fournisseurs d'identité FranceConnect actuellement recensés sont les sites suivants : impots.gouv.fr, ameli.fr et laposte.fr, cette liste pouvant être modifiée par FranceConnect.

Pour utiliser l'authentification FranceConnect, la Ville de Niort doit accepter l'ensemble des conditions d'utilisation dudit service par les fournisseurs de services

Il est demandé au Conseil municipal de bien vouloir :

- approuver l'utilisation de FranceConnect comme un des moyens de s'identifier pour utiliser les services numériques de la Ville de Niort ;
- approuver les conditions générales et les annexes pour les fournisseurs de services ci-annexées.

LE CONSEIL
ADOPTE

Pour :	43
Contre :	0
Abstention :	0
Non participé :	0
Excusé :	2

Pour le Maire de Niort,
Jérôme BALOGE
L'Adjoint délégué

Signé

Lucien-Jean LAHOUSSE

Direction interministérielle du numérique et des systèmes d'information et de communication

Conditions Générales d'Utilisation du service FranceConnect par les Fournisseurs de Services

Corps juridique

Novembre 2017

Table des matières

1. PREAMBULE

Ce document présente les modalités d'engagement à l'utilisation du téléservice FranceConnect (ci-après le « Service ») pour les partenaires qui offrent des services numériques (ci-après les « Fournisseurs de Services »). Il traduit les engagements de chacun en vue de faciliter et de simplifier la réalisation de démarches administratives pour les usagers. Il s'inscrit dans le cadre juridique :

- Du dispositif de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

- Du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

- De l'arrêté du 4 juillet 2013, pour les collectivités et leurs établissements, autorisant la mise en œuvre par les collectivités territoriales, les établissements publics de coopération intercommunale, les syndicats mixtes, les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou de plusieurs téléservices de l'administration électronique.

- De l'article 16A, de la loi n° 2000-321 du 12 avril 2000 modifiée relative aux droits des citoyens dans leurs relations avec les administrations, codifié aux articles L114-8 et suivants du Code des relations entre le public et l'administration.

- Le règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 (e-IDAS) sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

- De l'arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication (DINSIC) d'un téléservice dénommé « FranceConnect ».

Le service FranceConnect a pour ambition de fédérer les identités numériques des usagers et permettre :

- Aux usagers de bénéficier d'une véritable chaîne de confiance facilitant l'accès aux différents services numériques offerts, de permettre le suivi par l'usager des échanges de données le concernant, de garantir la confidentialité des informations et par conséquent, d'utiliser un même compte d'accès pour effectuer leurs démarches en ligne auprès de diverses entités en s'affranchissant de l'étape d'envoi de pièces justificatives transmises antérieurement.

- Aux Fournisseurs de Services de déléguer la gestion des identités numériques et l'authentification des usagers à des tiers de confiance Fournisseurs d'Identité.

2. OBJET DU DOCUMENT

Le présent document a pour objet de définir les conditions d'utilisation du téléservice FranceConnect, appelé ci-après le « Service » entre la DINSIC et les Fournisseurs de Services (FS).

Les présentes conditions générales d'utilisation s'organisent de la manière suivante :

- D'un document chapeau, le présent document ;

- D'annexes :
  - Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services ;
  - Annexe ii – Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect ;
  - Annexe iii – Annexe sécurité ;
  - Annexe iv – Annexe qualité de service et chaîne de support.

3. DEFINITIONS

Fournisseur de Services : sont Fournisseurs de Services, susceptibles d'adhérer au Service, les « autorités partenaires habilitées à traiter les démarches et formalités administratives des usagers en vertu d'un texte législatif ou réglementaire » au sens de l'article 4 de l'arrêté du 24 juillet 2015 précité.

Fournisseur d'Identité : fournisseur approuvé offrant des dispositifs d'identification et d'authentification vérifiés permettant aux usagers d'attester de leur identité dans le cadre de téléservices. Sont Fournisseurs d'Identité, susceptibles d'adhérer au Service, les personnes morales en mesure de :

- Respecter l'ensemble des critères exprimés dans la Convention d'adhésion au Service et ses annexes,
- Obtenir, auprès de l'ANSSI, la confirmation du respect des exigences du règlement e-IDAS applicables au niveau de garantie visé de ses moyens d'identification électronique (faible, substantiel et élevé). Cette obligation est réalisée à compter de la publication des modalités de labellisation et des organismes labellisés, y compris pour les Fournisseurs d'Identité déjà engagés dans le Service.

Fournisseur de Données : fournisseur disposant d'informations / de données concernant l'usager qui peuvent être transmises, avec le consentement au préalable de l'usager, aux Fournisseurs de Services via le Service.

Identité pivot : fait partie des données usagers fournies par les Fournisseurs d'Identité aux Fournisseurs de Services, via le Service, permettant d'identifier un usager particulier ou une entreprise.

Usager : personne physique qui utilise le Service via le site du Fournisseur de Services.

Utilisateurs : sont utilisateurs du Service les Fournisseurs de Données, les Fournisseurs d'Identité, les Fournisseurs de Services et les Usagers.

4. ROLES ET ENGAGEMENTS DE LA DINSIC

4.1. La DINSIC met en œuvre et opère le Service conformément au cadre juridique en vigueur défini en préambule.

4.2. La DINSIC procède au raccordement du Fournisseur de Services dans les conditions précisées dans l'Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services.

4.3. La DINSIC s'autorise à révoquer un Fournisseur de Services s'il estime que l'usage du Service porte préjudice à son image ou ne répond pas aux exigences de sécurité.

4.4. La DINSIC s'engage à transmettre les informations demandées par le Fournisseur de Services via le Service. Les catégories d'informations transmises et leurs conditions de traitement par le Fournisseur de Services sont définies dans l'Annexe ii – Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect.

4.5. La DINSIC s'engage à vérifier les informations d'identité reçues du Fournisseur d'Identité en faisant appel aux services de l'INSEE et, le cas échéant, à redresser l'identité de l'usager avant transmission des informations au Fournisseur de Services, conformément à l'Annexe ii – Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect.

4.6. La DINSIC s'engage à réaliser une recette d'implémentation avant chaque mise en service de FranceConnect par le Fournisseur de Services, conformément à l'Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services.

4.7. La DINSIC s'engage à ce que le Service FranceConnect soit accessible *a minima* aux mêmes conditions que celui du Fournisseur de Services. Les niveaux de service sont définis dans l'Annexe iv – Annexe qualité de service et chaîne de support.

4.8. La DINSIC s'engage à assurer la protection des données transmises dans le cadre du Service conformément à l'Annexe iii – Annexe sécurité, et aux mesures prévues par l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives et le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de cette ordonnance.

4.9. La DINSIC s'engage à assurer la traçabilité de toutes les actions réalisées par l'ensemble des utilisateurs du Service, y compris celles du Fournisseur de Services et de l'Usager, et à conserver ces informations conformément à l'article 6 de l'arrêté du 24 juillet 2015.

4.10. La DINSIC s'engage à fournir l'ensemble des ressources graphiques nécessaires à la mise en œuvre du dispositif par le Fournisseur de Services, conformément à l'Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services.

4.11. La DINSIC offre aux Fournisseurs de Services un support en cas d'incident ou d'alerte sécurité défini dans l'Annexe iv – Annexe qualité de service et chaîne de support.

4.12. La DINSIC s'engage à assurer le suivi et l'évaluation de l'utilisation du Service, et à communiquer les résultats obtenus aux Fournisseurs de Services.

5. ROLES ET ENGAGEMENTS DU FOURNISSEUR DE SERVICES

5.1. Le Fournisseur de Services s'engage à mettre en œuvre le Service conformément aux dispositions décrites dans l'Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services et l'Annexe ii - Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect et à implémenter l'ensemble des composants nécessaires à sa bonne utilisation.

5.2. Le Fournisseur de Services est responsable des traitements qu'il opère sur les données reçues au moyen du Service et, à ce titre, s'engage à effectuer toutes formalités préalables obligatoires auprès de la commission nationale de l'informatique et des libertés conformément à l'article 5 de l'arrêté du 24 juillet 2015. Il s'engage à ne pas commercialiser les données reçues, à ne pas les communiquer à des tiers en dehors des cas prévus par la loi. Il s'engage également à transmettre à la DINSIC, sur simple demande, le résultat de ces formalités.

5.3. Le Fournisseur de Services s'engage à assurer la pleine information de l'Usager sur les informations ou données nécessaires pour l'accomplissement de sa démarche, ainsi que celles qu'il se procure par l'intermédiaire du Service. Le Fournisseur de Services s'engage à recueillir, si cela s'avère nécessaire, le consentement exprès de l'Usager.

5.4. Le Fournisseur de Services s'engage à maintenir le Service conformément à l'Annexe iv – Annexe qualité de service et chaîne de support.

5.5. Le Fournisseur de Services s'engage à assurer la protection des données transmises dans le cadre du Service conformément à l'Annexe iii – Annexe sécurité.

5.6. Le Fournisseur de Services s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles définies dans l'Annexe iii – Annexe sécurité et à informer la DINSIC de toute difficulté de nature à compromettre le bon fonctionnement du Service.

5.7. Le Fournisseur de Services s'engage à mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment dans le cadre de la transmission de ces données au travers d'un réseau non sécurisé, ainsi que contre toute autre forme de traitement illicite.

5.8. Le Fournisseur de Services s'engage à être en mesure de retracer l'ensemble des transactions en rapport avec le Service et l'Usager.

5.9. Le Fournisseur de Services s'engage, le cas échéant, à répercuter les obligations en matière de sécurité et de confidentialité de données à caractère personnel aux éventuels prestataires ou sous-traitants ayant accès à ces données dans le cadre de l'administration, la maintenance et l'exploitation des services électroniques sous leur périmètre de responsabilité.

5.10. Le Fournisseur de Services s'engage à respecter les éléments graphiques ainsi que la charte FranceConnect, conformément à l'Annexe i – Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services.

5.11. Le Fournisseur de Services s'engage à respecter les critères d'accessibilité définis par le Référentiel Général d'Accessibilité pour les Administrations (RGAA) conformément à l'arrêté du 29 avril 2015, disponible à l'adresse suivante : http://references.modernisation.gouv.fr/accessibilite-numerique.

6. COUT DU SERVICE

6.1. Les coûts d'investissement et de fonctionnement du Service sont pris en charge par la DINSIC.

6.2. La participation au Service ne donne lieu à aucune compensation financière entre la DINSIC et le Fournisseur de Services.

7. ACCEPTATION – MODIFICATION – RESILIATION

7.1. La demande de raccordement du Fournisseur de Services, conformément à l'Annexe i – Annexe technique – Raccordement Processus d'implémentation de FranceConnect par le Fournisseur de Services, emporte acceptation des présentes conditions générales d'utilisation du Service.

7.2. Toute modification par la DINSIC des dispositions prévues par ce document, annexes comprises, fait l'objet d'une information aux Fournisseurs de Services.

7.3. Le Fournisseur de Services peut librement se désengager du Service en respectant un préavis de trois mois adressé par adresse mail à : support.partenaires@franceconnect.gouv.fr.

7.4. La DINSIC se réserve le droit de mettre un terme à la relation avec le Fournisseur de Services en cas de manquement aux présentes conditions générales d'utilisation non réparé à l'issue d'un délai maximum de 90 jours à compter d'une notification écrite au Fournisseur de Services.

8. RESPONSABILITES

8.1. La responsabilité de la DINSIC ne peut être engagée en cas d'usurpation d'identité ou de toute utilisation frauduleuse du Service.

8.2. La DINSIC est responsable des informations traitées dans le cadre du Service et, à ce titre, s'engage à respecter les obligations inhérentes à ce traitement, notamment celles relevant de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés et de l'arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect ».

8.3. Le Fournisseur de Services est responsable des informations reçues du Service et, à ce titre, s'engage à respecter les obligations inhérentes à leur traitement, notamment celles relevant de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés de l'arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect ».

8.4. Le Fournisseur de Services est responsable de tout manquement aux présentes Conditions générales d'utilisation du Service qui lui est imputable et peut donner lieu à résiliation dans les conditions prévues à l'article 7.4.

* * *

9. GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
DINSIC	Direction Interministérielle du Numérique et des Systèmes d'Information et de Communication
e-IDAS	electronic IDentification And Signature
FC	FranceConnect
FD	Fournisseur de Données
FI	Fournisseur d'Identité
FS	Fournisseur de Services
INSEE	Institut National de la Statistique et des Etudes Economiques
PSSI	Politique de Sécurité des Systèmes d'Information
RGS	Référentiel Général de Sécurité
SSI	Sécurité des Systèmes d'Information

Direction interministérielle du numérique et des systèmes d'information et de communication

Tour Mirabeau
39-43 quai André Citroën - 75015 Paris

www.franceconnect.gouv.fr

Direction interministérielle du numérique et des systèmes d'information et de communication

Conditions générales d'utilisation du service FranceConnect par les Fournisseurs de Services

Annexe i – Annexe technique – Processus d'implémentation de FranceConnect par le Fournisseur de Services

Novembre 2017

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

La présente annexe a pour objectif de définir les modalités de mise en œuvre de FranceConnect par le Fournisseur de Services en environnement d'intégration et de production. Elle s'inscrit en complément des Conditions Générales d'Utilisation du service FranceConnect par les Fournisseurs de Services et ne saurait être prise isolément.

2. PROCESSUS DE MISE EN ŒUVRE DE FRANCECONNECT

Le processus de mise en œuvre de FranceConnect par le Fournisseur de Services se décline en plusieurs étapes :

N°	Étapes	Engagements
1	**Inscription à FranceConnect et validation des CGU**	Obligatoire
2	**Intégration et configuration d'un client OpenID Connect**	Obligatoire
3	**Intégration d'un bouton d'action FranceConnect**	Obligatoire
4	**Intégration du "Kit FranceConnect"**	Facultatif
5	**Implémentation de la déconnexion**	Obligatoire
6	**Réconciliation et dissociation de compte**	Facultatif
7	**Gestion des erreurs entre FranceConnect et le Fournisseur de Services**	Obligatoire
8	**Expiration des données**	Obligatoire
9	**Respect de la charte**	Obligatoire
10	**Information auprès de la CNIL**	Obligatoire
11	**Recette et mise en production**	Obligatoire

2.1. Etape 1 – Inscription à FranceConnect et validation des CGU

Le Fournisseur de Services doit s'inscrire à FranceConnect via le formulaire d'enregistrement mis à sa disposition sur le portail FranceConnect.

Dans le cadre de la mise en œuvre le Fournisseur de Services se doit de s'enregistrer en précisant les informations suivantes :

Nom du service	Obligatoire
Email de contact	Obligatoire
Logo du service	Recommandé
Urls de callback *	Obligatoire - en y indiquant une par ligne
Quel est votre cas d'usage ?	Obligatoire

Concernant les URLs de callback :

- L'URL peut avoir une profondeur quelconque de sous domaines ;
- Le Fournisseur de Services peut utiliser des ports spécifiques ;

- Le Fournisseur de Services peut utiliser une IP plutôt qu'un FQDN préconisé (nom de domaine pleinement qualifié : adresse de nom de domaine entière, y compris le nom d'hôte, et le haut-niveau du domaine) ;
- Le « search » de l'URL peut être d'une taille arbitraire ;
- Le Fournisseur de Services peut utiliser « localhost » pour ses environnements de développement et de test.

Afin de valider son enregistrement, le Fournisseur de Services doit **accepter les conditions générales d'utilisation** (CGU) du service FranceConnect au moment de l'envoi de ses informations.

2.2. Etape 2 – Intégration et configuration d'un client OpenID Connect

FranceConnect suit l'implémentation standard d'OpenID Connect (OIDC).

Le protocole OpenID Connect est une surcouche d'identification au protocole OAuth 2.0. Il permet à un Fournisseur de Services d'accéder à l'Identité Pivot (cf. Annexe ii – Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect) des Usagers transmise par un Fournisseur d'Identité via l'intermédiaire de FranceConnect.

Le Fournisseur de Services est client OpenID Connect pour FranceConnect, ci-après le « Client » ou le « Fournisseur de Services ».
FranceConnect est fournisseur OpenID Connect pour le Fournisseur de Services.

Des informations complémentaires concernant OIDC sont disponibles aux adresses suivantes :

- Spécification du protocole : http://openid.net/connect/ ;
- Référence d'implémentation OpenID Connect : http://openid.net/specs/openid-connect-core-1_0.html.

2.2.1 Intégration

Le Fournisseur de Services doit implémenter et configurer un client OpenID Connect afin de communiquer avec FranceConnect.

Une liste non exhaustive de clients OpenID Connect est disponible à l'adresse suivante : http://openid.net/developers/libraries/.

2.2.2 Configuration

Le protocole OpenID Connect définit trois appels REST et un « endpoint » par le client OIDC (trois endpoints du côté fournisseur).

Les endpoints disponibles en environnement d'intégration en https sont les suivants :

Authorization	https://fcp.integ01.dev-franceconnect.fr/api/v1/authorize
Token	https://fcp.integ01.dev-franceconnect.fr/api/v1/token
UserInfo	https://fcp.integ01.dev-franceconnect.fr/api/v1/userinfo
Logout	https://fcp.integ01.dev-franceconnect.fr/api/v1/logout

2.2.2.1. Mise en place de la cinématique

Le Fournisseur de Services dans sa mise en œuvre doit suivre la cinématique suivante :

1. L'usager clique sur le bouton d'authentification du client.

2. Le Client fait une redirection vers le "authorization endpoint" de FranceConnect avec son client id et son url de callback.

<FC_URL>/api/v1/authorize [REDIRECTION]		
Description	**Contexte**	Le FS redirige depuis la requête précédente vers /api/v1/authorize pour engager la cinématique d'authentification.
	Origine ➔ Cible	FS ➔ FC
	Type d'appel	Redirection navigateur
Requête	**URL**	**<FC_URL>**/api/v1/authorize?response_type=code&client_id=**<CLIENT_ID>**&redirect_uri=**<FS_URL>**%2F<URL_CALLBACK>&scope=**<SCOPES>**&state=**<STATE>**&nonce= **<NONCE>**
	Méthode	GET
Réponse	/	

3. FranceConnect redirige alors l'usager vers sa mire d'authentification. Si l'Usager se connecte correctement, FranceConnect renvoie un code d'autorisation au Client.

<FS_URL>/<URL_CALLBACK> [REDIRECTION]		
Description	**Contexte**	L'internaute s'est identifié et authentifié sur le FI, FranceConnect redirige vers le callback du FS, avec un Authorization code dans l'URL.
	Origine ➔ Cible	FC ➔ FS
	Type d'appel	Redirection navigateur
Requête	**URL**	**<FS_URL>**/<URL_CALLBACK>?code=**<AUTHZ_CODE>**&state=**<STATE>**
	Méthode	GET
Réponse	/	

4. Le Client fait un appel Web service vers le "token endpoint" de FranceConnect avec le code d'autorisation reçu (**<AUTHZ_CODE>)**, et authentifie cette requête avec son client id et son client secret. FranceConnect retourne un « access token » (une chaîne de caractères encodée en base64), un « id token » (sous la forme d'un Json Web Token, voir https://developer.atlassian.com/static/connect/docs/concepts/understanding-jwt.html).

<FC_URL>/api/v1/token [WEB SERVICE]		
Description	**Contexte**	Le FS a récupéré un authorization code. Il veut maintenant récupérer un access token et un id token.
	Origine ➔ Cible	FS ➔ FC

	Type d'appel	Appel de Web service
Requête	**URL**	**<FC_URL>**/api/v1/token
	Méthode	POST
	Corps HTTP	'grant_type': 'authorization_code', 'redirect_uri': '**<FS_URL>**/<URL_CALLBACK>', 'client_id': '**<CLIENT_ID>**', 'client_secret': '**<CLIENT_SECRET>**', 'code': '**<AUTHZ_CODE>**'
Réponse	**Corps HTTP**	{ 'access_token': **<ACCESS_TOKEN>**, 'token_type': 'Bearer', 'expires_in': 3600, 'id_token': **<ID_TOKEN>** }

5. Le Client fait un appel Web service vers le "userInfo endpoint" de FranceConnect avec l'« access token » reçu.

<FC_URL>/api/v1/userinfo [WEB SERVICE]		
Description	Contexte	Le FS a récupéré un access token. Il veut maintenant récupérer les USER INFO.
	Origine ➔ Cible	FS ➔ FC
	Type d'appel	Appel de Web service
Requête	URL	<FC_URL>/api/v1/userinfo?schema=openid
	Méthode	GET
	Entêtes HTTP	Authorization = 'Bearer <ACCESS_TOKEN>'
Réponse	Corps HTTP	<USER_INFO>

6. FranceConnect renvoie les informations de l'usager au Client. La description des informations transmises est définie dans l'Annexe Echange de données entre FranceConnect et le Fournisseur de services.

2.2.2.2. Diagramme des flux

Le schéma ci-après fournit le diagramme des flux entre l'usager, le Fournisseur de Services et France Connect.

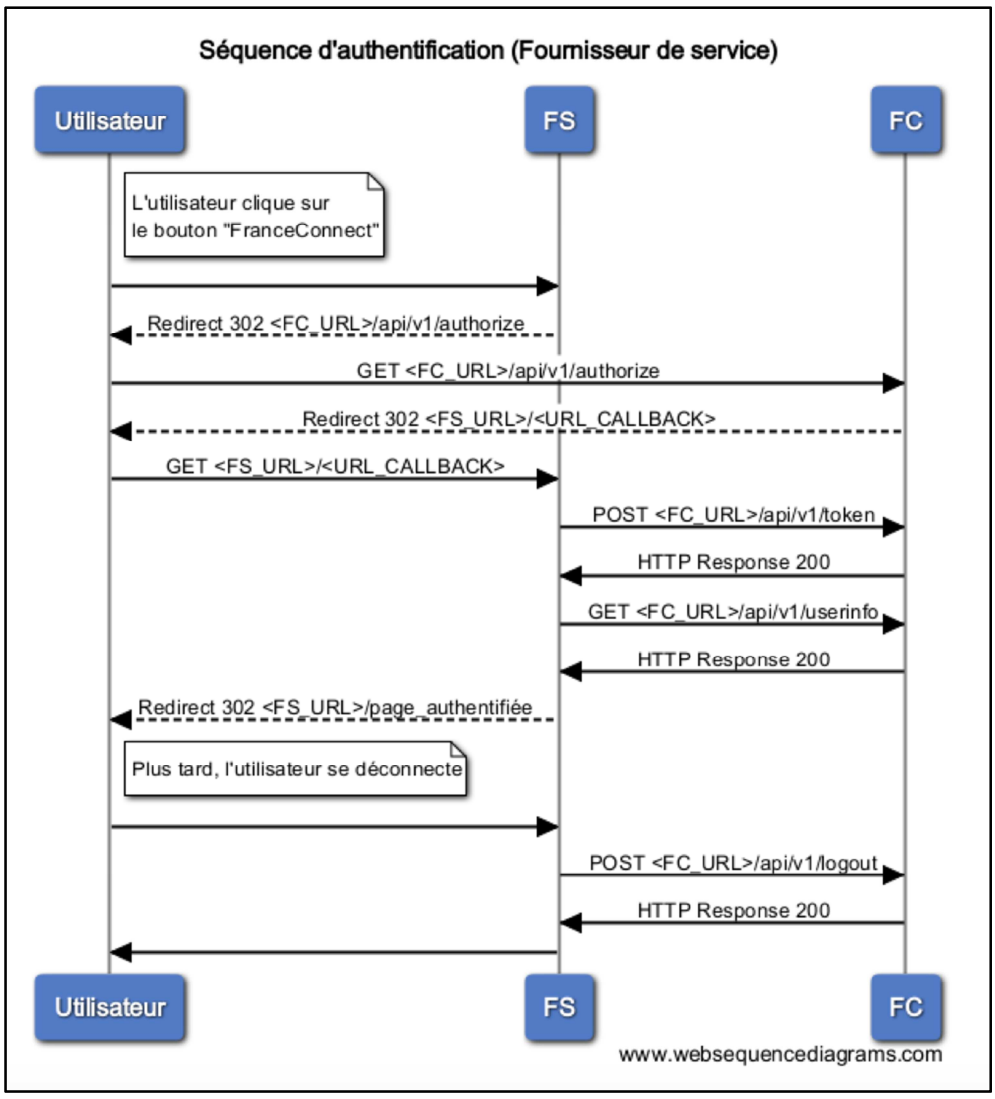

Figure 1 : Diagramme des flux « Usager ⟷ Fournisseur de Services ⟷ FranceConnect »

2.3. Etape 3 – Intégration d'un bouton d'action FranceConnect

Les boutons d'action FranceConnect sont primordiaux dans l'usage du service. Contrairement au logo, ils ne sont pas représentatifs mais actifs. Afin d'accéder au service, il est obligatoire d'utiliser l'un des boutons proposés par la charte graphique prévue au paragraphe « 2.9. Etape 9 – Respect de la charte » de la présente annexe et aucun autre visuel. Ces boutons sont disponibles sur le portail développeur.

Figure 2 : Boutons d'action FranceConnect

Les boutons sont toujours accompagnés du texte « Se connecter avec FranceConnect », en le rajoutant au besoin.

Quel que soit le bouton d'action choisi pour proposer la connexion à **FranceConnect**, le Fournisseur de Services doit obligatoirement s'accompagner d'un lien précisant « Qu'est-ce que FranceConnect ? » pointant vers l'url suivante pour l'intégration : https://fcp.integ01.dev-franceconnect.fr/a-propos (une url de production sera fournie dès validation de la recette).

Dans le choix de bouton, le Fournisseur de Services doit prendre garde à ne pas utiliser :

- Des couleurs de boutons qui soient les mêmes que celles du fond utilisé ;
- Des couleurs de boutons qui soient foncées avec un fond foncé sur le site ;
- Des liens vers « Qu'est-ce que FranceConnect ? » qui soient également trop proches de la couleur de fond.

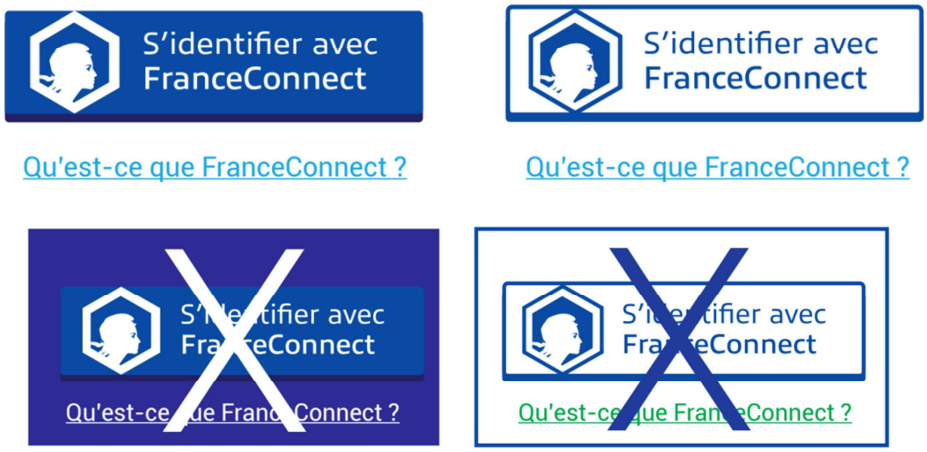

Figure 3 : Intégration FranceConnect OK / KO

2.4. Etape 4 – Intégration du « Kit FranceConnect »

Le « Kit FranceConnect » est le script permettant au Fournisseur de Services de disposer du bouton de déconnexion ainsi que du lien vers les traces de connexion.
Il est nécessaire que l'Usager soit connecté à FranceConnect pour afficher ce bloc.

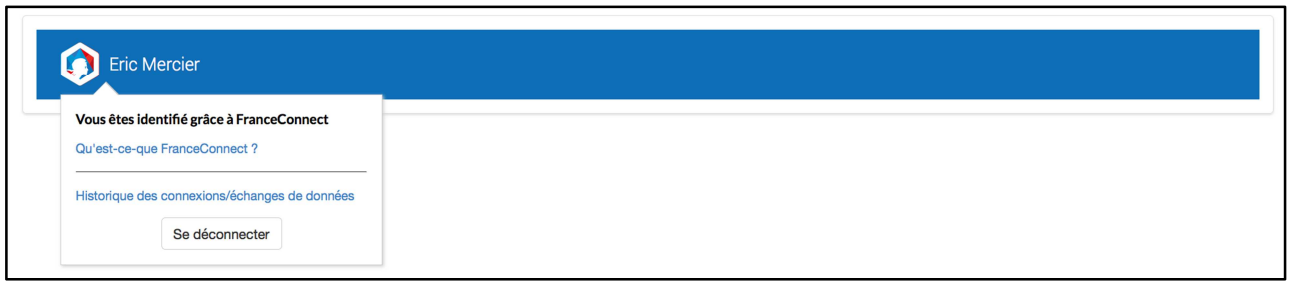

Figure 4 : Kit FranceConnect

La DINSIC recommande l'intégration du kit FranceConnect en :

1. Incluant la librairie javascript FranceConnect en bas de page :

```
<script src="http://fcp.integ01.dev-franceconnect.fr/js/franceconnect.js"></script>
```

2. Insérant dans le code HTML la structure suivante :

```
<div id="fconnect-profile" data-fc-logout-url="/lien-deconnexion">
   <a href="#"> le nom de l'utilisateur connecté* </a>
</div>
```

3. Paramétrant les variables suivantes :

Variables	**Valeurs**
data-fc-logout-url	Mettre le lien de déconnexion
Utilisateur	Remplacer par le nom de l'utilisateur connecté

En fonction des contraintes du Fournisseur de Services, il est possible que ce dernier veuille intégrer le kit manuellement. Dans ce cas, le Fournisseur de Services met en place :

- Un lien vers l'historique des connexions et des échanges de données (traces) ;

Environnement	**URLs**
Intégration	https://fcp.integ01.dev-franceconnect.fr/traces

- La déconnexion FranceConnect (Section 4 de la présente annexe) ;
- Un lien vers la page « Qu'est-ce que FranceConnect? » ;

Environnement	**URLs**
Intégration	https://fcp.integ01.dev-franceconnect.fr/a-propos

2.5. Etape 5 – Implémentation de la déconnexion

FranceConnect implémente la section sur la déconnexion, en cours de spécification dans la norme OpenID Connect : http://openid.net/specs/openid-connect-session-1_0-15.html#RPLogout.

Le Fournisseur de Services doit proposer la déconnexion de FranceConnect à son usager et implémenter la cinématique suivante :

1. L'Usager clique sur un lien de déconnexion présenté par le Fournisseur de Services. « Il est rappelé que le bouton de déconnexion est présent dans le kit d'intégration FranceConnect ».

2. Le Fournisseur de Services doit **déconnecter** l'Usager de son application, puis le rediriger vers la page de déconnexion de FranceConnect : ***<FC_URL>/api/v1/logout***. L'Usager choisit de se déconnecter ou non du Service FranceConnect.

Figure 5 : Page de déconnexion de FranceConnect

3. L'Usager est redirigé vers la page de retour spécifiée par le Fournisseur de Service.

Le Fournisseur de Services doit préciser l'URL de redirection de l'Usager via le paramètre ***post_logout_redirect_uri***, ainsi que transmettre l'**id_token** récupéré lors de l'authentification de l'Usager via le paramètre **id_token_hint**.

Il est obligatoire de renseigner les différentes urls de redirections de déconnexion dans les paramètres client OIDC.

<FC_URL>/api/v1/logout [REDIRECTION]		
Requête :	**URL :**	**<FC_URL>**/api/v1/logout?id_token_hint=**<ID_TOKEN_HINT>** &state=**<STATE>**&post_logout_redirect_uri=**<POST_LOGOUT_REDIRECT_URI>**
	Méthode :	GET

2.6. Etape 6 – Réconciliation et dissociation de compte

La DINSIC recommande de mettre en œuvre la réconciliation et la dissociation des comptes existants des Usagers du Fournisseur de Services. L'implémentation est propre au Fournisseur de Services en fonction de son système d'information.

2.7. Etape 7 – Gestion des erreurs entre FranceConnect et le Fournisseur de Services

FranceConnect peut renvoyer des messages d'erreurs au Fournisseur de Services. Pour ce faire, FranceConnect passe par le mécanisme de retour d'erreurs d'un Fournisseur d'Identité openid connect tel que décrit dans la norme OIDC (http://openid.net/specs/openid-connect-core-1_0.html#AuthError, en particulier les sections 3.1.2.6 (authentification), 3.1.3.4 (jeton d'accès) et 5.3.3 (service d'informations utilisateur)).

2.8. Etape 8 – Expiration des données

FranceConnect gère plusieurs types de données « périssables » lors d'une authentification par OpenID Connect ou de la fourniture d'un jeton d'accès à une ressource protégée fournie par un Fournisseur de Données (cinématique OAuth2 classique). Chacune de ces données possède une durée de vie qui lui est propre au-delà de laquelle elle doit être régénérée :

Type	**Usage**	**Durée**
Session Web	A chaque authentification et pour maintenir la session côté FranceConnect	30 minutes sans action
Access Token	Récupération d'informations (phase 3 cinématique d'authentification / cinématique OAuth2)	20 minutes
Authorization code	Code fourni lors du début de la démarche d'authentification, il sert ensuite à récupérer l'access token	5 minutes

2.9. Etape 9 – Respect de la charte

2.9.1 Orthographe

FranceConnect s'écrit avec les deux caractéristiques immuables suivantes :

- Tout attaché et sans le moindre espace, FranceConnect se compose de 13 caractères ;
- FranceConnect a deux Capitales et onze bas-de-casses :
    - Le F initial est une Majuscule ainsi que le C ;
    - Les autres caractères sont en minuscules.

Note : il n'y a que dans le logo que les deux parties du mot FranceConnect sont détachées (cf. 2.9.2 Le logo).

2.9.2 Le logo

Le logo type FranceConnect se compose d'un symbole hexagonal à facettes bleu, blanc et rouge. L'hexagone représente la France, son unité. Il est utilisé uniquement à des fins de représentation. Le choix se fait librement parmi les logos disponibles dans la charte.

Il n'est jamais utilisé :

- Comme bouton d'action de connexion ;
- Partiellement ou juste en sigle, s'il s'agit de représenter FranceConnect.

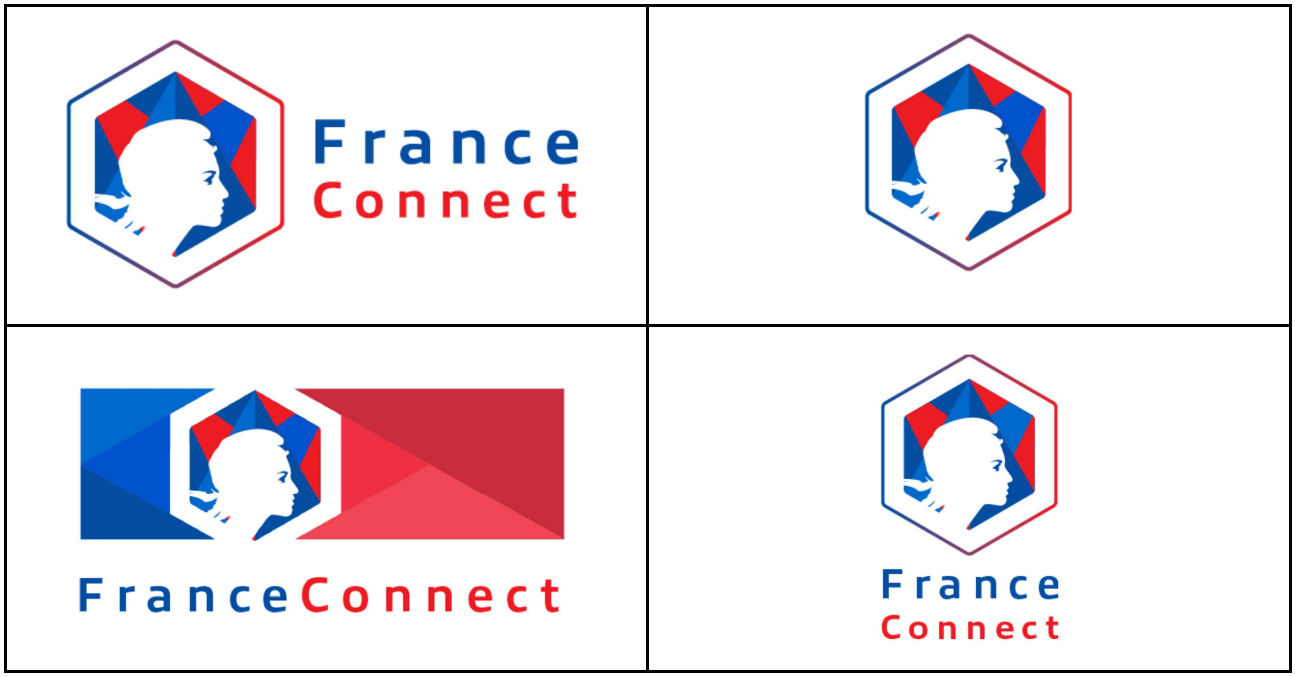

Figure 6 : Logos FranceConnect

2.9.3 Les couleurs

Pour être valides au test d'accessibilité AA, les couleurs ci-dessous sont utilisées avec la police par défaut « Roboto » en blanc (R255 V255 B255, #FFFFFF) :

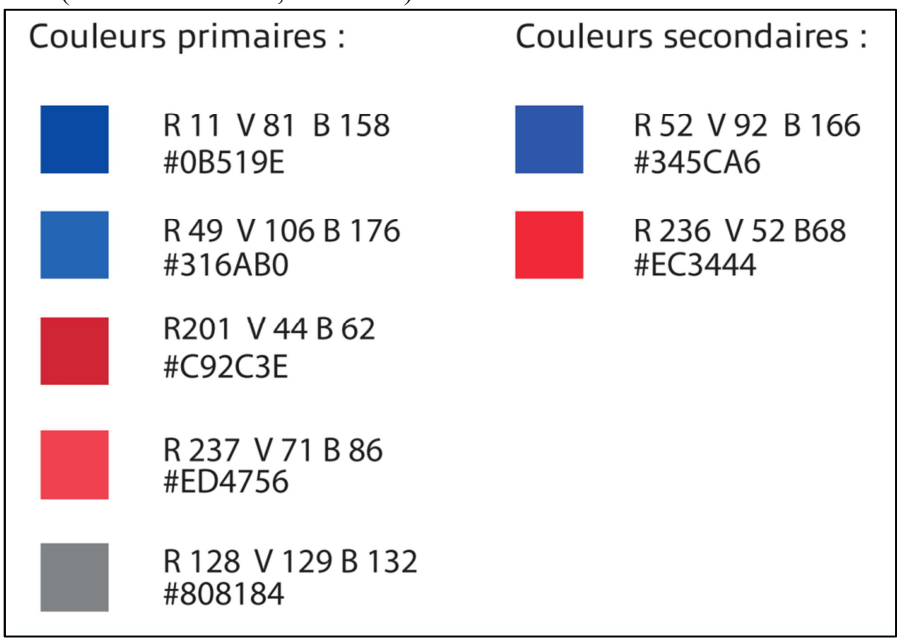

Figure 7 : Couleurs valides au test d'accessibilité AA

2.9.4 La police

La police « Roboto » est la police utilisée par FranceConnect. Elle est disponible gratuitement sur GoogleFont aux formats TrueType et OpenTrueType.
La police du logo est Allumi de Jean-François Porchez (2011).

2.10. Etape 10 – Déclaration CNIL de conformité à FranceConnect

Avant sa mise en production, le Fournisseur de Services doit effectuer une déclaration CNIL de conformité à FranceConnect.

2.11. Etape 11 – Renseignement de la Fiche Contacts FranceConnect - Partenaire

Avant sa mise en production, le Fournisseur de Services doit renseigner la Fiche Contacts FranceConnect – Partenaire avec ses contacts.

2.12. Etape 12 – Recette et mise en production

Pour sa mise en production, le Fournisseur de Services doit en faire la demande par email (support.partenaires@franceconnect.gouv.fr) à la DINSIC et fournir :

- La demande de la déclaration de conformité à FranceConnect qui figure dans l'accusé réception de la CNIL ;
- Le numéro de déclaration qui figure dans le récépissé ;
- La Fiche Contacts FranceConnect – Partenaire ;
- La demande de la déclaration de conformité à FranceConnect qui figure dans l'accusé réception de la CNIL ;
- Le numéro de déclaration qui figure dans le récépissé ;

- La Fiche Contacts FranceConnect – Partenaire ;
- L'URL de callback de connexion ;
- L'URL de callback de logout ;
- Le mail du destinataire du client_id ;
- Le numéro de téléphone portable du destinataire du client_secret (transmis par sms) ;
- Les coordonnées de votre support ;
- Le ou les adresses emails des destinataires des statistiques d'utilisations du bouton dans votre outil ;
- Le logo qui s'affichera dans la mire FranceConnect (format png/svg ou jpeg, taille minimum 55*70 – attention à la lisibilité) ;
- La date de mise en production souhaitée par le Fournisseur de Services.

La DINSIC réalise une recette du dispositif. La DINSIC peut également demander un audit réalisé par un prestataire choisi par la DINSIC sur la partie du système d'information concernée (brique d'authentification).

Après validation de la recette, l'équipe support communique au Fournisseur de Services, par deux canaux distincts obligatoirement, les informations de production suivantes :

- Par mail :
    - Client_id ;
    - Authorize ;
    - Token : https://app.franceconnect.gouv.fr/api/v1/token ;
    - UserInfo : https://app.franceconnect.gouv.fr/api/v1/userinfo ;
    - Logout ;
    - A propos de FranceConnect ;
- Par SMS :
    - Client_secret.

3. SUPPORT

FranceConnect met à disposition du Fournisseur de Services l'adresse électronique suivante : support.partenaires@franceconnect.gouv.fr pour tout besoin relatif à la mise en œuvre de FranceConnect. Le détail des moyens de support et de maintenance mis en œuvre pour assurer la qualité du service est par ailleurs présenté dans l'annexe iv – Annexe qualité de service et chaîne de support.

4. GLOSSAIRE

AUTHZ_CODE	Code retourné (dans l'URL) par FC au FS lorsque ce dernier fait un appel sur le endpoint FC_URL/api/v1/authorize. Il est ensuite passé (dans le corps de la requête HTTP POST) lors de l'appel sur le endpoint FC_URL/api/v1/token
ACCESS_TOKEN	Token retourné (dans le corps HTTP) par l'appel au endpoint FC_URL/api/v1/token. Il est ensuite passé (dans l'URL) lors de l'appel au endpoint FC_URL/api/v1/userinfo
CALLBACK_URL_DATA	Le callback du FS, communiqué lors de son inscription auprès de FC
CGU	Conditions Générales d'Utilisation
CLIENT_ID	Identifiant du FS, communiqué lors de son inscription auprès de FC
CLIENT_SECRET	Le secret du FS, communiqué lors de son inscription auprès de FC
FC_URL	URL de FranceConnect
FS_URL	Votre URL, en tant que Fournisseur de Services
FQDN	Fully Qualified Domain Name
ID_TOKEN	ID_TOKEN Objet JWT retourné par l'appel au endpoint FC_URL/api/v1/token. L'objet JWT est un objet JSON formatté et signé. Le JSON doit contenir ces cinq clés : aud,exp,iat,iss,sub. Exemple : {'aud':'895fae591ccae777094931e269e46447', 'exp':1412953984, 'iat':1412950384, 'iss':http://franceconnect.gouv.fr, 'sub':YWxhY3JpdMOp, 'idp':'dgfip', 'nonce':'12344354597459'}. Détail des champs : ● aud, exp, iat, iss, sub : ce sont des champs obligatoires de la norme OpenIDConnect ● nonce : paramètre obligatoirement envoyé lors de l'appel à /authorization. Le FS doit impérativement vérifier que la valeur correspond bien à celle qu'il a envoyée, et qui doit être liée à la session de l'utilisateur ● idp : spécifique à FranceConnect. Fournit l'identifiant du fournisseur d'identité utilisé par l'utilisateur courant (exemple: 'dgfip' si l'utilisation a choisi d'utiliser son compte des Finances Publiques). Si vous utilisez une librairie pour transformer le json en JWT, il génèrera une chaîne de caractères constitué de 3 chaînes base64 séparées par un point. Pour vérifier la signature, il faut utiliser le secret partagé avec FranceConnect (qui vous a été attribué lors de votre provisioning côté FC)
ID_TOKEN_HINT	Objet JWT identique au format ID_TOKEN qui a été reçu lors de l'échange avec l'appel à FC_URL/api/v1/token et doit être passé en paramètre lors de l'appel à FC_URL/api/v1/logout
NONCE	Champ obligatoire, généré aléatoirement par le FS que FC renvoie tel quel dans la réponse à l'appel à /token, pour être ensuite vérifié par le FS. Il est utilisé pour empêcher les attaques par rejeu

POST_LOGOUT_REDIRECT_URI	L'URL de redirection après la demande de déconnexion FC
SCOPES	Liste des scopes demandés séparés par des espaces (donc par %20 au format unicode dans l'URL). Voici la liste supportée par FranceConnect ● openid : obligatoire, permet de demander l'identifiant technique de l'utilisateur au formatOpenIDConnect ● profile : obligatoire, permet de récupérer l'essentiel de l'identité pivot. Si disponible, renvoie aussi le preferred_username ● birth : obligatoire, permet de récupérer la ville et le département de naissance de la personne (identité pivot) ● email : facultatif, si disponible, renvoie l'adresse e-mail de la personne ● address : facultatif, si disponible, renvoie l'adresse postale de la personne ● phone : facultatif, si disponible, renvoie le numéro de téléphone de la personne Cette liste de scopes est définie par la norme OpenIDConnect L'identité pivot complète se récupère par deux scopes différents (profile + birth) car les informations de ville et de département de naissance de la personne ne font pas partie des données pouvant être renvoyées en soumettant le scope 'profile' seul. Le découpage est fait ici dans un souci de se conformer à la norme.
STATE	Champ obligatoire, généré aléatoirement par le FS, que FC renvoie tel quel dans la redirection qui suit l'authentification, pour être ensuite vérifié par le FS. Il est utilisé afin d'empêcher l'exploitation de failles CSRF
SUB	Identifiant technique (unique et stable dans le temps pour un individu donné) fourni par FranceConnect au FS. Le sub est présent dans l'IdToken retourné au FS ainsi que dans les informations d'identité. Le sub retourné par FranceConnect est spécifique à chaque Fournisseur de Services (i.e: Un usager aura toujours le même sub pour un FS donné, en revanche il aura un sub différent par FS qu'il utilise).
USER_INFO	Voir l'Annexe ii – Annexe technique - Echange de données entre le Fournisseur de Services et FranceConnect

Direction interministérielle du numérique et des systèmes d'information et de communication

Tour Mirabeau
39-43 quai André Citroën - 75015 Paris

www.franceconnect.gouv.fr

Direction interministérielle du numérique et des systèmes d'information et de communication

Conditions générales d'utilisation du service FranceConnect par les Fournisseurs de Services

Annexe technique – Echange de données entre le Fournisseur de Services et FranceConnect

Novembre 2017

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

Cette annexe définit les données échangées entre FranceConnect et le Fournisseur de Services et la manière dont celles-ci sont traitées. Elle s'inscrit en complément des Conditions Générales d'Utilisation du service FranceConnect par les Fournisseurs de Services et ne saurait être prise isolément.

2. DEFINITION DE L'IDENTITE PIVOT

Le dispositif FranceConnect permet aux Usagers d'utiliser les télé-services offerts par des Fournisseurs de Services après s'être identifiés et authentifiés auprès d'un Fournisseur d'Identité.

FranceConnect met en œuvre pour ce faire la cinématique du protocole OpenID Connect dite par « code autorisation » qui permet la vérification de l'identité de l'Usager, son authentification et l'échange des données qui constituent cette identité.

L'ensemble de ces données d'identité est dénommé « Identité pivot ». Cette identité est transmise par FranceConnect au Fournisseur de Services, après vérification de son existence et de son unicité auprès du Répertoire National d'Identification des Personnes Physiques (RNIPP).

3. CONSTITUTION DE L'IDENTITE PIVOT

Chaque donnée constituant l'identité pivot d'un Usager est appelée **scope**. Des **alias** sont également à disposition du Fournisseur de Services lui permettant de récupérer un ensemble de scopes.
Le scope **<openid>** doit obligatoirement être récupéré par le Fournisseur de Services. Le Fournisseur de Services est libre de récupérer les autres scopes en fonction des informations dont il a besoin. Le Fournisseur de Services doit récupérer uniquement les informations nécessaires au cadre des démarches proposées.

Certains scopes sont "optionnels" : ils ne seront pas obligatoirement transmis bien que le Fournisseur de Services en ait fait la demande. En effet, ces données sont transmises par le Fournisseur d'Identité que si ce dernier possède ces informations.

Les données vérifiées (en opposition avec les données déclaratives) sont les données qui ont été corrigées suite à l'interrogation du RNIPP par FranceConnect.

La liste des scopes est définie par la norme OpenID Connect : http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims et leur implémentation pour FranceConnect est décrite dans le tableau suivant :

ALIAS	SCOPES	FORMAT	DESCRIPTION	TYPE	STANDARD OIDC
	openid	string	Identifiant technique (sub) de l'utilisateur au format OpenID Connect	Obligatoirement demandé par le FS Non vérifié	OUI
profile	**given_name**	string	Prénoms de la personne, séparés par des espaces selon le standard OpenID Connect	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	OUI
	family_name	string	Nom de naissance de la personne	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	OUI
	preferred_username	string	Nom d'usage de la personne	Optionnellement demandé par le FS Optionnellement transmis par FC Vérifié auprès du RNIPP	OUI

	gender	string	Sexe de la personne, male / female	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	OUI
	birthdate	string	Date de naissance de la personne, au format YYYY-MM-DD	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	OUI
birth	**birthcountry**	string	Pays de naissance de la personne, au format code INSEE	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	NON
	birthplace	string	Ville de naissance de la personne, code INSEE du lieu de naissance ou chaîne vide si la personne est née à l'étranger	Optionnellement demandé par le FS Obligatoirement transmis par FC Vérifié auprès du RNIPP	NON
	email	string	Adresse e-mail de la personne	Optionnellement demandé par le FS Obligatoirement transmis par FC Non vérifié	OUI
	address	string	Adresse postale de la personne, chaîne de caractères restituée telle qu'elle a été transmise par le Fournisseur d'Identité. Aucune règle de gestion n'est adressée au Fournisseur d'Identité quant au format de cette donnée.	Optionnellement demandé par le FS Optionnellement transmis par FC Non vérifié	OUI

	phone	string	Numéro de téléphone de la personne, chaîne de caractères restituée telle qu'elle a été transmise par le Fournisseur d'Identité. Aucune règle de gestion n'est adressée au fournisseur d'identité quant à la restitution de cette donnée.	Optionnellement demandé par le FS Optionnellement transmis par FC Non vérifié	OUI

4. RECUPERATION DE L'IDENTITE PIVOT

1. Le Fournisseur de Services après avoir récupéré un accès token (cf. Annexe i - Annexe technique – Raccordement / Processus d'implémentation de FranceConnect par le Fournisseur de Services) va récupérer les USER_INFO de l'Usager en faisant un appel de web service <FC_URL>/api/v1/userinfo à FranceConnect.

Url de la requête :

<FC_URL>/api/v1/authorize?response_type=code&client_id= **<CLIENT_ID>**&redirect_uri= **<FS_URL>**%2F<URL_CALLBACK>&scope=**<SCOPES>**&state=**<STATE>**&nonce= **<NONCE>**

2. FranceConnect effectue un appel de web service similaire au Fournisseur d'Identité afin de récupérer de son côté les USER_INFO de l'Usager.

3. Après récupération des USER_INFO auprès du Fournisseur d'Identité, FranceConnect effectue un appel au RNIPP afin de vérifier l'identité de l'Usager transmise par le Fournisseur d'Identité. Le RNIPP est un instrument de vérification de l'état civil des personnes maintenu par l'Institut National de la Statistique et des Etudes Economiques (INSEE[1]).

4. FranceConnect peut ensuite ajuster les attributs de l'identité reçue du Fournisseur d'Identité afin de les aligner avec l'identité retournée par le RNIPP avant leur transmission au Fournisseur de Services.
    - Si l'appel au RNIPP renvoie une identité, alors celle-ci est utilisée par FranceConnect afin de corriger les attributs d'identité transmis par le Fournisseur d'Identité en cas de valeurs divergentes. Tous les champs suivants sont susceptibles d'être corrigés :
        - Le(s) prénom(s) ;
        - Le(s) nom(s) ;
        - La date de naissance ;
        - Le lieu de naissance ;
        - Le sexe.

      Le seul champ de l'identité pivot qui n'est pas corrigé suite à l'appel au RNIPP est le « preferred_username » (nom d'usage). L'INSEE ne renvoie pas le nom d'usage, mais seulement le nom de naissance. Cependant, le RNIPP est capable de retrouver une identité à partir d'un nom d'usage.
      Si l'identité renvoyée indique que la personne est décédée, l'authentification est rejetée et tracée.
      En cas de doublon (deux Usagers ayant la même identité pivot), l'Usager ne pourra pas se connecter du fait de l'impossibilité d'obtenir l'unicité de son Identité pivot.
    - Si l'appel au RNIPP ne renvoie pas d'identité, l'authentification est bloquée : FranceConnect n'est pas en capacité de contrôler l'identité.

Remarques :

- Les codes retour transmis par l'INSEE suite à un appel au RNIPP :
    - Demande identifiée sans divergence d'état civil ;
    - Demande identifiée avec divergence(s) d'état civil ou NIR ;

[1] http://www.insee.fr/fr/themes/detail.asp?ref_id=fd-etatcivil2010&page=fichiers_detail/etatcivil2010/presentation.htm

  - Demande non identifiée mais existence d'un seul écho ;
  - Demande non identifiée mais existence de plus d'un écho ;
  - Demande identifiée avec le nom d'usage uniquement ;
  - Demande non identifiée sans écho ;
  - Demande rejetée au contrôle en raison d'erreurs de syntaxe ;

- L'appel au RNIPP et ses résultats sont bloquants pour tous les Fournisseurs d'Identité. Si l'identité a été contrôlée ou validée par le RNIPP, alors l'identité de l'INSEE sera utilisée à la place de l'identité renvoyée par le Fournisseur d'Identité.

- Les erreurs renvoyées par le RNIPP sont bloquantes (personne non trouvée, identité non redressée, personne décédée) : l'Usager est renvoyé vers la mire d'authentification, avec un message d'erreur l'invitant à se connecter avec un autre Fournisseur d'Identité.

5. GENERATION DE LA CLE DE HACHAGE

FranceConnect se sert des données redressées / corrigées **(USER_INFO)** pour générer une clé de hachage unique pour l'Usager. Cette clé de hachage générée via un algorithme SHA-256 est stockée en base de données chez FranceConnect.

FranceConnect va également générer un sub aléatoire. Ce sub correspond au scope **<openid>** transmis au Fournisseur de Services pour la création ou réconciliation de compte.
FranceConnect va également associer le couple sub généré / client_id du Fournisseur de Services à cette clé de hachage. Un sub est unique par Usager pour un Fournisseur de Services donné.

6. DUREE DE CONSERVATION DES DONNEES

Les données constituant l'identité pivot ne sont pas stockées en base de données par FranceConnect, ces données sont sauvées en session côté serveur pendant une durée de 30 minutes.

Les données sont récupérées par FranceConnect à chaque connexion de l'Usager.

FranceConnect conserve les trente-six mois d'historique de connexion de l'Usager dans un fichier de logs et indexé via un moteur ElasticSearch.

En l'absence de connexion de l'usager pendant une durée de trente-six mois, les données stockées en base (clé de hachage, couples client_id/sub) sont supprimées.

Direction interministérielle du numérique et des systèmes d'information et de communication

Tour Mirabeau
39-43 quai André Citroën - 75015 Paris

www.franceconnect.gouv.fr

Direction interministérielle du numérique et des systèmes d'information et de communication

Conditions générales d'utilisation du service FranceConnect par les Fournisseurs de Services

Annexe iii – Annexe sécurité

Novembre 2017

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

La présente annexe a pour objet de décrire les exigences et recommandations de sécurité relatives aux échanges entre FranceConnect et les Fournisseurs de Services, tous deux désignés comme « les Parties » dans la suite du document.

Elle rappelle en outre les engagements attendus en matière de protection des données à caractère personnel, de confidentialité et de respect du Référentiel Général de Sécurité (RGS).

Elle s'inscrit en complément des Conditions Générales d'Utilisation du service FranceConnect par les Fournisseurs de Services et ne saurait être prise isolément.

2. EXIGENCES RELATIVES AU FOURNISSEUR DE SERVICES

2.1. Exigences de sécurité relatives au protocole OpenID Connect

Le Fournisseur de Services met en œuvre les mesures de sécurité techniques et organisationnelles nécessaires afin d'assurer, sur son périmètre :

- La non divulgation des données fonctionnelles et techniques échangées dans le cadre du protocole à un tiers non autorisé ;
- La mise en place de mesures afin de prévenir leur fuite en cas d'intrusion ;
- La confidentialité et l'intégrité des secrets échangés (mots de passe, clés cryptographiques).

Le Fournisseur de Services répond par ailleurs aux exigences suivantes :

- Mettre en œuvre les mesures de sécurité nécessaires afin d'assurer le stockage sécurisé du secret permettant l'authentification du client OpenID Connect.
- Générer le paramètre *state* aléatoirement en utilisant une fonction de génération de caractères aléatoires sécurisée et avec une entropie équivalente à 100 bits (minimum 16 caractères avec un alphabet de 70 caractères différents). Le paramètre *state* transmis dans la requête de demande d'autorisation est obligatoire afin de contrer les attaques CSRF. Il est retransmis dans les paramètres de l'URL de retour et sa concordance doit être vérifiée avec la valeur stockée dans la session de l'utilisateur.
- Valider systématiquement toutes les données en entrée, si possible par l'utilisation de listes blanches, pour empêcher par exemple leur manipulation en insérant des caractères spécifiques, en particulier, valider les codes d'autorisation, les jetons d'accès et le contenu de l'identité pivot (user_info).
- Générer le paramètre *nonce* aléatoirement en utilisant une fonction de génération de caractères aléatoires sécurisée et une entropie équivalente à 100 bits (minimum 16 caractères avec un alphabet de 70 caractères différents). Le paramètre *nonce* transmis dans la requête de demande d'autorisation est obligatoire afin de contrer le rejeu de requête. Il est retransmis dans le jeton nommé token_id retourné par FranceConnect lors de la récupération du jeton d'accès. Sa concordance doit être vérifiée avec la valeur stockée dans la session de l'utilisateur.
- Vérifier le haché d'authentification grâce au secret du jeton d'authentification token_id et les informations qu'il contient :
    - Le paramètre « aud » doit contenir le client_id,
    - Le paramètre « exp » correspondant à l'expiration de l'authentification ne doit pas être expiré,
    - Le paramètre « nonce » doit correspondre à celui fourni dans la requête de demande d'authentification,
    - Le paramètre « iss » doit contenir le nom de domaine de France Connect,
    - Le paramètre « acr » doit contenir le niveau eIDAS précédemment fourni lors de la requête d'authentification et conservé avec la session de l'utilisateur.
- Vérifier le nom de domaine du serveur retourné avec celui utilisé pour l'appel serveur à serveur (appel FS ←→FD).

2.2. Veille et sensibilisation

Le Fournisseur de Services met en œuvre sur son périmètre une veille avancée afin de détecter les velléités d'attaques cyber criminelles sur les services en lien avec FranceConnect (FC). En cas d'attaque, il s'engage à alerter FranceConnect et l'ensemble des partenaires de la chaîne de sécurité.

Le Fournisseur de Services forme et sensibilise les acteurs sous son autorité à la sécurité et aux enjeux de FranceConnect (notamment les développeurs et à la cible les agents utilisant FC).

2.3. Recommandations globales quant à l'implémentation sécurisée des services numériques

Il est recommandé au Fournisseur de Services de s'appuyer sur les recommandations ANSSI pour la sécurisation des applications web (note technique No DAT-NT-009/ANSSI/SDE/NP), en particulier :

- Appliquer les principes de défense en profondeur aux architectures logicielles et matérielles des applications. La mise en œuvre de ses principes par des mesures adéquates est à étudier dès l'étape de conception, au vu des risques et menaces auxquels sera exposée l'application.
- Sécuriser le processus d'administration via des protocoles sécurisés et restreindre les tâches d'administration aux seuls postes d'administration dûment authentifiés et habilités.
- Appliquer le principe du moindre privilège à l'ensemble des éléments du système (« tout ce qui n'est pas autorisé explicitement est par défaut interdit »).
- Contrôler systématiquement les données en entrée des requêtes, qu'elles soient fonctionnelles ou techniques et quel que soit leur provenance.

3. EXIGENCES RELATIVES A FRANCECONNECT

3.1. Conformité réglementaire

Le service FranceConnect a fait l'objet d'une déclaration auprès de la CNIL (Délibération 2015-254 du 16 juillet 2015). Parallèlement, une démarche d'homologation de sécurité a été engagée par la DINSIC.

3.2. Mesures de sécurité

FranceConnect met en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin de protéger les données traitées et stockées dans le cadre du service, et ce au regard des objectifs de sécurité identifiés suite à l'analyse des risques de sécurité. Ces mesures concernent en particulier :

- Le contrôle systématique de tous les paramètres en entrée des requêtes afin de réduire le risque d'injection. FranceConnect met en œuvre des mécanismes de blocage des clients en cas d'échecs répétés afin d'éviter les attaques par force brute. Cette mesure peut aller jusqu'à la déconnexion d'un fournisseur en cas de menace critique.
- La robustesse des secrets, leur stockage et leur transmission sécurisés ainsi que leur renouvellement régulier.
- De manière générale : l'application des principes de défense en profondeur, notamment en matière de gestion des droits d'accès aux différents composants du système (reverse proxies, serveurs d'application et de données, etc.).

3.3. Gestion des incidents

FranceConnect offre aux Fournisseurs de Services un support en cas d'incident, conformément à l'Annexe iv - Annexe qualité de service et chaîne de support.

4. GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
DINSIC	Direction Interministérielle du Numérique et des Systèmes d'Information et de Communication
FC	FranceConnect
FD	Fournisseur de Données
FI	Fournisseur d'Identité
FS	Fournisseur de services
PSSI	Politique de Sécurité des Systèmes d'Information
RGS	Référentiel Général de Sécurité
SSI	Sécurité des Systèmes d'Information

Direction interministérielle du numérique et des systèmes d'information et de communication

Tour Mirabeau
39-43 quai André Citroën - 75015 Paris

www.franceconnect.gouv.fr

Direction interministérielle du numérique et des systèmes d'information et de communication

Conditions générales d'utilisation du service FranceConnect par les Fournisseurs de Services

Annexe iv – Annexe qualité de service et chaîne de support

Novembre 2017

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

Cette annexe a pour objet de décrire les moyens mis en œuvre par la DINSIC pour assurer aux Fournisseurs de Services de FranceConnect une qualité de service satisfaisante. Pour ce faire, elle présente les processus de maintenance et support de FranceConnect ainsi que les taux de disponibilité du service.

Elle s'inscrit en complément des Conditions Générales d'Utilisation du service FranceConnect par les Fournisseurs de Services et ne saurait être prise isolément.

2. DESCRIPTION DE SERVICES

Le présent document décrit les services dont bénéficie le Fournisseur de Services dans le cadre du support et de la maintenance applicative et technique FranceConnect.

Les prestations des équipes FranceConnect comprennent :

- **La maintenance FranceConnect** : les moyens mis en œuvre dans le cadre de cette prestation permettent de traiter les anomalies applicatives et les évolutions nécessaires pour le fonctionnement de FranceConnect selon l'état de l'art et les normes européennes (règlement « eIDAS »).
- **Le support FranceConnect** : les moyens mis en œuvre dans le cadre de cette prestation offrent un support de différents niveaux aux Fournisseurs de Services.

2.1. Maintenance FranceConnect

La DINSIC prend en charge :

- La correction des anomalies applicatives ;
- Et les évolutions nécessaires au dispositif FranceConnect.

L'application FranceConnect est conçue de sorte que les maintenances applicatives puissent être effectuées sans interruption de service. Cependant, la DINSIC s'engage à régler les anomalies bloquantes dans les 4h après prise en compte de l'anomalie.

La DINSIC n'assure pas la maintenance des applications, des équipements et des infrastructures localisés chez les Fournisseurs de Services et chez les Usagers.

Toute modification applicative ou d'infrastructure fait l'objet d'une information préalable de la DINSIC dans un délai de six mois pour permettre aux Fournisseurs de Services de prendre leur disposition.

2.2. Support FranceConnect

2.2.1 Support et assistance aux Usagers

Il est à la charge du Fournisseur de Services de mettre en place le support auprès des Usagers (email, téléphone, formulaire de contact, etc.) afin de leur fournir assistance. Aucune demande émanant des Usagers n'est traitée par l'équipe support FranceConnect.

Une base de connaissance enrichie et maintenue par l'équipe support FranceConnect est à la disposition du Fournisseur de Services afin de l'aider dans la résolution des problèmes ou demandes d'aide de l'Usager. La base de connaissance est accessible à tous sous réserve de création d'un compte. Sans solution du Fournisseur de Services, seuls les contacts autorisés sont en mesure d'interagir avec l'équipe support FranceConnect.

La liste des contacts autorisés à contacter l'équipe support FranceConnect doit être communiquée par le Fournisseur de Services lors de la transmission des identifiants pour mise en production. Dans le cas où le Fournisseur de Services prévoit un « Single Point Of Contact », ce dernier sera en charge de contacter l'équipe support FranceConnect en cas de besoin.

2.2.2 Support et assistance aux Fournisseurs de Services

Il est de la responsabilité du Fournisseur de Services de s'adapter aux évolutions éventuelles du dispositif FranceConnect, que celles-ci soient liées ou non au protocole OIDC (OpenID Connect). Pour cela, le Fournisseur de Services doit s'inscrire à la liste de diffusion FranceConnect (https://franceconnect.gouv.fr/fs-diffusion) afin d'être informé de ses évolutions et des implémentations à mettre en œuvre le cas échéant.

Le centre de support FranceConnect assure une assistance aux Fournisseurs de Services de 9h30 à 18h (du lundi au vendredi). Pour cela, le Fournisseur de Services crée une demande d'assistance (ouverture d'un ticket) via un outil dont l'accès lui sera communiqué par FranceConnect.

Dès réception de la demande du Fournisseur de Services par le centre de support FranceConnect, un personnel qualifié s'engage à répondre dans les 48h ouvrées suivant le constat et l'analyse des faits.

Chaque ticket client est référencé par un numéro unique et associé à un niveau de sévérité suite au diagnostic effectué par le support FranceConnect.

Niveaux de priorité des incidents			Sévérité
Périmètre Impact	Dysfonctionnement concernant l'ensemble des applications du Fournisseur de Services utilisant FranceConnect	Entreprise	1 (Critique)
	Dysfonctionnement concernant une seule application du Fournisseur de Services utilisant FranceConnect	Site	2 (Majeure)
	Dysfonctionnement touchant plusieurs Usagers	Plusieurs Usagers	3 (Moyenne)
	Dysfonctionnement ne touchant qu'un Usager	Usager	4 (Mineure)
	Demande d'information autour du fonctionnement de FranceConnect	Informations	5 (Info)

Figure 1 : Niveaux de sévérité d'un ticket

Après affectation du niveau de sévérité, l'équipe support doit résoudre l'incident suivant un temps imparti. Néanmoins, chaque niveau de sévérité possède une échéance qui donnera lieu à une escalade si le problème n'est toujours pas résolu.

NIVEAU DE SEVERITE	DESCRIPTION	ESCALADE APRES	TEMPS TOTAL DE TRAITEMENT EN HEURES OUVREES	ESCALADE VERS
1 (Critique)	- Le système ne fonctionne plus. - Le service n'est plus assuré. - Le service ne peut être relancé sans la résolution complète et définitive du problème. - Un problème de sécurité.	1 heure	2 heures	Responsable de la production
2 (Majeure)	- Le système est opérationnel mais ne fonctionne que grâce aux dispositifs des systèmes de secours. - Les temps de réponse sont fortement affectés.	2,5 heures	4 heures	Équipe Support de niveau 3

3 (Moyenne)	- Le service est opérationnel mais présente des réductions de fonctionnalités ou des dysfonctionnements. - Les temps de réponse sont fortement dégradés.	8 heures	12 heures	Équipe Support de niveau 2
4 (Mineure)	- Les fonctionnalités majeures du service ne sont pas touchées. - Aucun dysfonctionnement critique n'existe mais les temps de réponse peuvent être partiellement affectés avec des fonctionnalités pouvant apparaître de façon réduite au vu du Client.	15 heures	24 heures	Équipe Support de niveau 1
5 (Info)	- Le service fonctionne parfaitement. - La question ne concerne pas un dysfonctionnement de l'application FranceConnect. - Il s'agit simplement d'une demande d'information de la part d'un usager, ou de la part d'un fournisseur (services, identités ou données).	15 heures	24 heures	Équipe Support de niveau 1

Figure 2 : Escalade et temps imparti au traitement d'un incident en fonction de sa sévérité

2.2.3 Conditions de fermeture d'un ticket

Les conditions de fermeture d'un ticket sont les suivantes :

- Une demande d'assistance (ticket) sera fermée par la DINSIC si celle-ci est résolue avec la confirmation verbale ou écrite du Fournisseur de Services.
- Un ticket pour un objet non résolu sera fermé si les deux parties en conviennent par écrit.
- Un ticket sera fermé par la DINSIC, au bout de 48h ouvrées en cas d'absence de réactivité ou de non-collaboration du Fournisseur de Services à fournir les informations nécessaires permettant sa résolution.
- Un ticket sera fermé par la DINSIC lorsque celui-ci sera résolu par la DINSIC, notifié au Fournisseur de Services et sans remarque de ce dernier.

3. GARANTIE DE DISPONIBILITE ET QUALITE DE SERVICE

La DINSIC met en œuvre les moyens nécessaires pour assurer des performances et une disponibilité optimale du dispositif FranceConnect.

La DINSIC, en raison de l'évolution technologique, se réserve le droit de faire évoluer à tout moment le présent document en informant le Fournisseur de Services de la ou des modification(s) et ce, à condition d'un maintien ou d'une amélioration du niveau de qualité de service.

Le taux de disponibilité annuel du dispositif est de 99,5% : l'ensemble des applicatifs est déployé en haute disponibilité, avec des équilibreurs qui assurent la répartition de charge.

L'indisponibilité est caractérisée par les éléments suivants :

- FranceConnect n'affiche pas la mire de choix des Fournisseurs d'Identité.
- FranceConnect n'est pas en mesure de renvoyer les données d'identité demandées par le Fournisseur de Services alors que l'authentification a réussi chez le Fournisseur d'Identité.
- Tous les Fournisseurs d'Identité sont indisponibles alors même que FranceConnect fonctionne toujours.

4. INDICATEUR DE MESURE DE LA QUALITE DU SERVICE

Outre les moyens mis en place pour garantir la haute disponibilité du service FranceConnect, la DINSIC procède au suivi des incidents d'exploitation (y compris les incidents de sécurité) et alimente un indicateur rendant compte de la qualité des réponses aux incidents et anomalies.

Description du service	Le service comprend le traitement des incidents et des anomalies	
Couverture du service	➢ Service HO : les plages de service comprennent des plages fixes du lundi au vendredi de 9H30 à 18H ➢ Pas de service en HNO	
Niveaux de service		
Description de l'indicateur	**Niveau de service**	**Règle de gestion**
Pourcentage des incidents d'exploitation résolus	95% en moins de 24 heures ouvrées	∑ incidents résolus par le centre de support FranceConnect en moins de 24 h ouvrées / ∑ incidents escaladés au centre de support FranceConnect

Direction interministérielle du numérique et des systèmes d'information et de communication

Tour Mirabeau
39-43 quai André Citroën - 75015 Paris

www.franceconnect.gouv.fr